Event Management Automation Protocol (EMAP) – Draft Use Cases and Requirements

Paul Cichonski (NIST)
George Saylor (G2)

High Level Goals of EMAP

- Expand the effectiveness of the NIST Security Automation Program by establishing a suite of specifications standardizing the communication of digital event data.
  - EMAP will be a peer of the Security Content Automation Protocol (SCAP).
  - Relationships between the boundary objects in SCAP and EMAP domains will be captured.
- Develop and implement an EMAP Validation Program that will ensure compliance with EMAP specifications and increase the effectiveness of procurement decisions within organizations.

EMAP Workflow Components (1 of 3)

EMAP Component	EMAP Enabled ?	Component Type	Description
Event Producer	Maybe	Product Capability	Any producer of events (may produce records of events in standard or proprietary formats).
Proprietary Event Data	No	Data Exchange Format	Any non-standard record of an event.
Event Parser	Yes	Product Capability	Parses proprietary event records to produce standardized event records.
Event Parsing Rules	Yes	Data Exchange Format	Standardized rules telling parser how to convert from one format to another.
Standardized Event Record	Yes	Data Exchange Format	Standards-based record of a specific event.
Event Store	Yes	Product Capability	Stores event data from disparate sources.

** Components are broken apart for illustrative purposes. Vendors will likely group multiple components into one tool.*

EMAP Workflow Components (2 of 3)

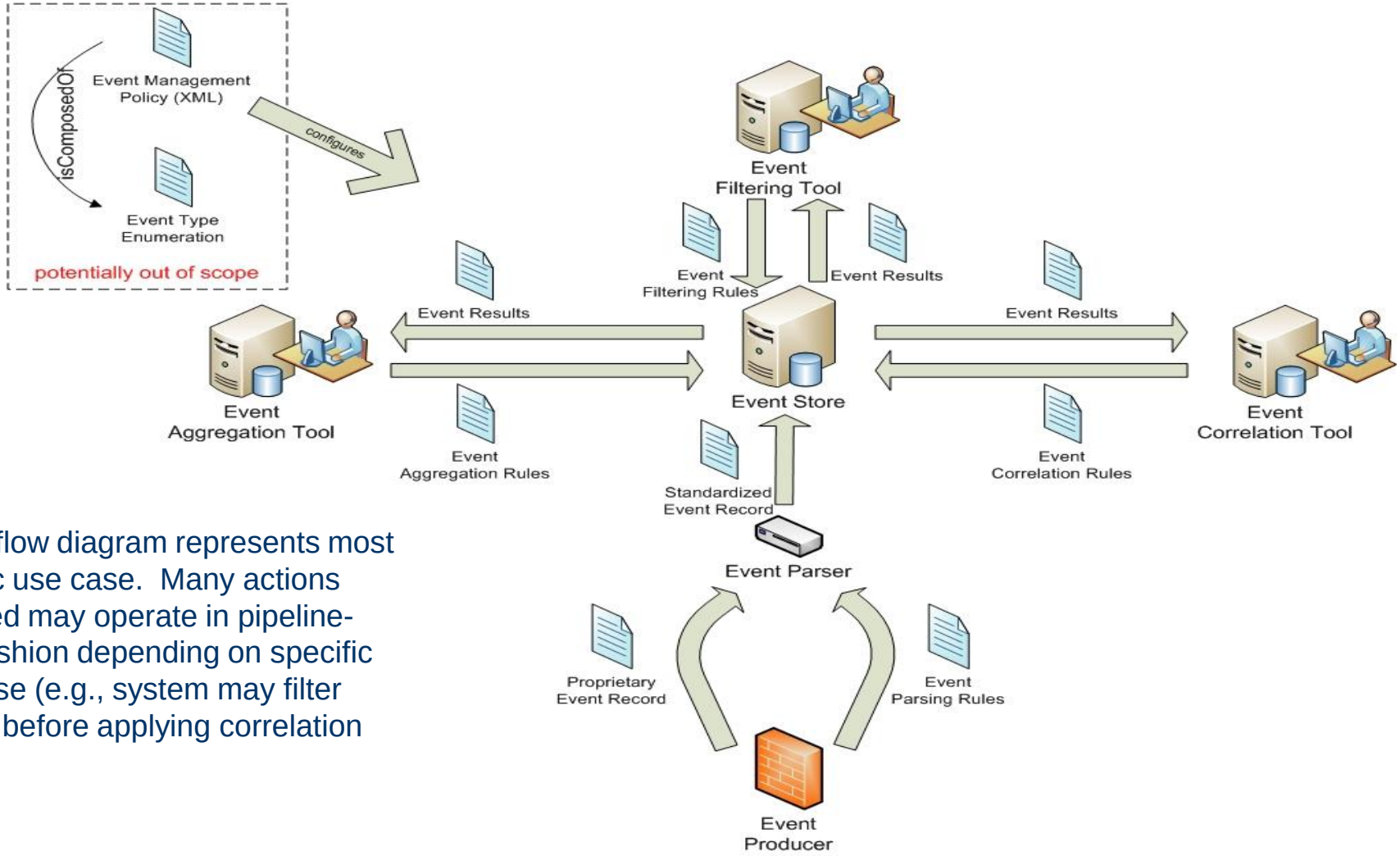
EMAP Component	EMAP Enabled ?	Component Type	Description
Event Correlation Tool	Yes	Product Capability	Tool that allows a user to correlate event data.
Event Correlation Rules	Yes	Data Exchange Format	Rules describing how to correlate event data. Boundary objects like CVE would likely relate to a rule describing the events produced when the CVE is exploited (e.g, through relationship: “exploitShownBy”).
Event Results	Yes	Data Exchange Format	Set of event results matching specific set of rules/query.
Event Filtering Tool	Yes	Product Capability	Tool that allows a user to filter events.
Event Filtering Rules	Yes	Data Exchange Format	Rules describing how events should be filtered.
Event Aggregation Tool	Yes	Product Capability	Tool that allows user to aggregate sets of events across some user-defined criteria.
Event Aggregation Rules	Yes	Data Exchange Format	Rules describing how to aggregate event data.

EMAP Workflow Components (3 of 3)

EMAP Component	EMAP Enabled ?	Component Type	Description
Event Management Policy	Maybe Potentially out of scope*	Data Exchange Format	Event / Audit Management Policy must be expressed in a machine readable format to enable automation. Language for expressing this policy must capture the following (at a minimum): 1) Type of events to log 2) Types of systems to log 3) Types of users to log 4) Attributes of events to log 5) Frequency / retention of logging.
Event Type Enumeration	Maybe Potentially out of scope*	Data Exchange Format	An enumeration of the high-level disparate types (or categories) of events. Event Management Policy languages may use items from this enumeration set to identify types of events to log (e.g., see PCI section 10.2 and 10.3 for example types).

** These components may be fulfilled by other areas within the Security Automation Program.*

EMAP Generic Workflow



- Workflow diagram represents most generic use case. Many actions depicted may operate in pipeline-type fashion depending on specific use case (e.g., system may filter events before applying correlation rules).

Use Case 1 – Audit Management

- An internal employee's actions have become suspect and the organizations audit management has been tasked with identifying any activity that would corroborate existing evidence. Using an EMAP compliant audit management tool that supports a *Standardized Event Record* syntax and *Event Correlation Rules* an analyst is able to quickly create queries for searching historical employee audit data. The organization may later use these same rules for alerting on any future employee activity considered anomalous to their job function. The organization may also choose to share these rules with partner organizations.

Workflow for use case 1 (audit management)

Step	Actor	Description	EMAP Component(s)
1	Malicious User	User conducts suspicious activity on internal network. This activity produces event records.	- Event Producer - Standardized Event Record
2	Audit Management Analyst	Analyst models the suspicious activity and atomic events that comprise it. Analyst also creates EMAP rules to search for similar activity within the network.	- Standardized Event Record - Event Filtering Rules - Event Correlation Rules
3	Audit Management Analyst	Analyst runs EMAP rules against event data repository to discover if similar activity has occurred in the past.	- Event Filtering Tool - Event Correlation Tool - Event Store - Event Results
4	Audit Management Analysis	Analyst places new rule in internal knowledge repository (not currently an EMAP component). System may continuously run rules captured in knowledge repository against event store to prevent identified activity in the future. This provides a mechanism for making incident history data actionable.	- Event Filtering Rules - Event Filtering Tool - Event Correlation Rules - Event Correlation Tool

Use Case 2 – Regulatory Compliance

- Event management regulations and policy (e.g., PCI 10.2 and 10.3) normally specifies the types of events, users, and systems to capture log data from. Policy also specifies frequency of logging, and retention time for log data. An event management team may use EMAP-expressed policy data to automatically configure their event management systems. Also, If the log data is EMAP compliant, then the auditor will be able to easily collect the data and verify compliance with policy using standardized queries.

Workflow for use case 2 (regulatory compliance)

Step	Actor	Description	EMAP Component(s)
1	Policy Writer	Create high-level event management policy, written in natural language (NL).	N/A
2	Technical Policy Writer	Translate NL policy into machine readable format that captures: 1) Type of events to log 2) Types of systems to log 3) Types of users to log 4) Attributes of events to log 5) Frequency / retention of logging.	- Event Management Policy - Event Type Enumeration
3	Event Management Team	Ensure event producers produce correct type of event data, and that event data is stored according to policy. Ideally this process could be automated if EMAP compliant tools understand XML policy.	- All EMAP components

Use Case 3 – Incident Handling

- Various agencies across the Federal Government are witnessing malicious activity across their respective networks. Along with government agencies, major companies in the private sector are also witnessing similar activity. Individuals from a few of companies publish initial *Event Correlation Rules,* for identifying the attack. As new information on the attack becomes available, other end users offer additional contributions and incremental improvements are made to the rules. Using vetted community input as a starting point, US-CERT develops and tests *Event Correlation Rules*, which it then shares within the Federal Government and private sector. Although institutions such as DoD, FDA, and USDA have implemented and support separate SIEM correlation technologies, each organizations' solution is EMAP complaint. Subsequently, each organization is able to utilize US-CERT's published rule set. The Federal Government now has reasonable assurance in the uniformity and coverage of its detective capabilities across EMAP compliant organizations.

Workflow for use case 3 (incident handling)

Step	Actor	Description	EMAP Component(s)
1	Federal Agency	Agency identifies incident within internal networks. Agency then captures events associated with incident and reports data to US-CERT.	- Event Producer - Standardized Event Record
2	US-CERT	US-CERT works with reporting agency, and other interested parties to model the incident and atomic events that comprise it. US-CERT then creates EMAP rules based on this model.	- Standardized Event Record - Event Filtering Rules - Event Correlation Rules
3	US-CERT	US-CERT disseminates incident report containing EMAP rules.	- Event Filtering Rules - Event Correlation Rules
4	Federal Agencies	All agencies within government scan EMAP compliant event stores to determine if incident is occurring on their networks.	- Event Filtering Tool - Event Correlation Tool - Event Store - Event Results

Use Case 4 – Event Filtering

- One government agency may wish to share information with another government agency. The agency adheres to government-wide digital access control policy that specifies that all event information may be shared, except the source and destination IP addresses. The digital access control policy provides EMAP-expressed machine readable filtering rules that the agency may use to scrub the sensitive information from the event data prior to sharing with the other organization.

Workflow for use case 4 (event filtering)

Step	Actor	Description	EMAP Component(s)
1	Policy Writer	Create high-level digital access control policy relating to event data sharing between organizations.	N/A
2	Technical Policy Writer	Creates standardized event filtering rules that agencies may use to automate digital access control enforcement.	- Event Management Policy - Event Filtering Rules
3	Event Management Team	Ensure event stores only provide external access through channels that enforce digital access control policy using standards-based filtering rules that will work on any EMAP-compliant vendor solution.	- Event Store - Event Filtering Rules - Event Filtering Tool - Event Results

Use Case 5 – Digital Forensics

- During legal disputes, forensic examiners will often rely on digital event records as a source of evidence to prove/disprove their claims. However, digital event logs must adhere to certain standards relating to log integrity and chain of custody for logs to be admissible in a court of law. If an *Event Producer* is required to comply with these standards, they may need to ensure that log data is digitally signed. Also, any intermediary systems wishing to augment log data (e.g., to add tagging metadata) must do so in a way that does not break the chain of custody. This means that intermediary systems must ensure that modifications to log records do not invalidate original digital signatures. A *Standardized Event Record* specification must provide mechanisms for maintaining log integrity and chain of custody. Leveraging this standardized mechanism, forensic examiners may use the same method for proving log integrity across a wide variety of EMAP compliant event logs.

Workflow for use case 5 (digital forensics)

Step	Actor	Description	EMAP Component(s)
1	Event Producer	Event Producer produces event logs and applies digital signatures to log records. This digital signature may be applied at either individual event record level, or at collection level, depending on processing/integrity requirements.	- Event Producer - Standardized Event Record
2	Intermediary System	Intermediary system processes log data from event producer before it is accepted into Event Store. The Intermediary system appends tagging metadata to log records, while maintaining chain of custody. Log data is then passed to Event Store.	- Standardized Event Record - Event Store (note: concept of intermediary system not currently captured in generic workflow diagram)
3	Forensic Examiner	Forensic examiner queries Event Store for incident-specific activity. All Event Results adhere to legal standards for admissibility in court.	- Event Store - Event Filtering Rules - Event Filtering Tool - Event Correlation Rules - Event Correlation Tool - Event Results

Use Case 6 – EMAP Adoption in Legacy Environments

- The success of event management automation is largely dependent on the ease of adoption within an organization. Organizations that adopt EMAP will likely have a variety of legacy *Event Producers* that will generate log data according to a proprietary syntax and not support the EMAP *Standardized Event Record* syntax. In these cases, the organization may create *Event Parsing Rules* that will run in an EMAP compliant *Event Parser*. These *Event Parsing Rules* will instruct the parser on how to translate *Proprietary Event Data* into the *Standardized Event Record* syntax. Through this modular approach organizations may begin to leverage EMAP without the need to update all legacy software within their network. In addition, since these rules will run in any EMAP compliant *Event Parser,* organizations may share these rules with partner organizations, or upload them to public repositories promoting community collaboration.

Workflow for use case 6 (EMAP Adoption in Legacy Environments)

Step	Actor	Description	EMAP Component(s)
1	Event Management Analyst	Analyst identifies software within the network that does not produce EMAP compliant Standardized Event Data. Analyst then writes EMAP Event Parsing Rules instructing an Event Parser on how to translate proprietary event data syntax to standardized syntax (e.g., Apache WWW format to CEE format).	- Event Producer - Event Parsing Rules
2	Event Management Analyst	Analyst then configures the Event Parser to use the specific translation rules when processing event data from specific Event Producers (e.g., in this case all Apache WWW servers).	- Event Producer - Event Parsing Rules - Event Parser
3	Event Parser	Event parser translates all proprietary event record data from proprietary syntax to standardized syntax. Parser then passes standardized event record data to Event store for additional processing.	- Event Parsing Rules - Event Parser - Standardized Event Record - Event Store
4	Organization	Organization uploads new standardized Event Parsing Rules to public repository promoting open collaboration.	- Event Parsing Rules

EMAP Derived Requirements (1 of 3)

I. Definition of a common data model for event record data
   a) Must define common vocabulary for event attributes.
   b) Must allow common event attributes to be shared across disparate event types and disparate types of event producers.
   c) Must allow disparate types of event producers to customize event attributes.
   d) Must allow events to be modified in a way that does not break chain of custody or the integrity of the original event.

II. Definition of one, or more expressions for event data exchange.
   a) Must allow for digital signing of one or multiple events.

III. Definition of a mechanism for mapping proprietary event data exchange expression to standardized event data exchange expression.

EMAP Derived Requirements (2 of 3)

IV. Definition of an exchange format for event correlation rules.
   a) Must provide ability to correlate events across disparate event types and across disparate types of event producers.

V. Definition of an exchange format for event filtering rules.
   a) Must provide ability to filter events across disparate event types and across disparate types of event producers.

VI. Definition of an exchange format for event aggregation rules.
   a) Must provide ability to filter events across disparate event types and across disparate types of event producers.

VII. Definition of a generic result interchange format for responding to machine queries of an event store.

EMAP Derived Requirements (3 of 3) (possibly out of scope*)

VIII. Definition of a policy language for expressing event management policy.
   a) Must allow for capturing policy relating to the type of events to log
   b) Must allow for capturing policy relating to the types of systems to log
   c) Must allow for capturing policy relating to the types of users to log
   d) Must allow for capturing policy relating to the attributes of events to log
   e) Must allow for capturing policy relating to the frequency / retention of logging.

IX. Method for uniquely identifying high-level event types.

** These requirements may be fulfilled by other areas within the Security Automation Program.*

EMAP Workflow Components mapped to derived requirements (1 of 3)

EMAP Component	EMAP Enabled?	Description	Derived Requirement
Event Producer	Maybe	Any producer of events (may produce records of events in standard or proprietary formats).	I, II
Proprietary Event Data	No	Any non-standard record of an event.	N / A
Event Parser	Yes	Parses proprietary event records to produce standardized event records.	I, II, III
Event Parsing Rules	Yes	Standardized rules telling parser how to convert from one format to another.	I, II, III
Standardized Event Record	Yes	Standards-based record of a specific event.	I, II
Event Store	Yes	Stores event data from disparate sources.	I, II

EMAP Workflow Components mapped to derived requirements (2 of 3)

EMAP Component	EMAP Enabled?	Description	Derived Requirement
Event Correlation Tool	Yes	Tool that allows a user to correlate event data.	IV
Event Correlation Rules	Yes	Rules describing how to correlate event data. Boundary objects like CVE would likely relate to a rule describing the events produced when the CVE is exploited (e.g, through relationship: “exploitShownBy”).	IV
Event Results	Yes	Set of event results matching specific set of rules/query.	VII
Event Filtering Tool	Yes	Tool that allows a user to filter events.	V
Event Filtering Rules	Yes	Rules describing how events should be filtered.	V
Event Aggregation Tool	Yes	Tool that allows user to aggregate sets of events across some user-defined criteria.	VI
Event Aggregation Rules	Yes	Rules describing how to aggregate event data.	VI

EMAP Workflow Components mapped to derived requirements (3 of 3)

EMAP Component	EMAP Enabled ?	Description	Derived Requirement
Event Management Policy	Maybe Potentially out of scope	Event / Audit Management Policy must be expressed in a machine readable format to enable automation. Language for expressing this policy must capture the following (at a minimum): 1) Type of events to log 2) Types of systems to log 3) Types of users to log 4) Attributes of events to log 5) Frequency / retention of logging.	VIII
Event Type Enumeration	Maybe Potentially out of scope	An enumeration of the high-level disparate types (or categories) of events. Event Management Policy languages may use items from this enumeration set to identify types of events to log (e.g., see PCI section 10.2 and 10.3 for example types).	IX

Proposed EMAP Specifications to satisfy derived requirements

Specification Acronym	Specification Name	Derived Requirement	EMAP Component
CEE	Common Event Expression	I, II	Standardized Event Record
OEEL	Open Event Expression Language	III	Event Parsing Rules
CERE	Common Event Rule Exchange	IV, V, VI	- Event Correlation Rules - Event Filtering Rules - Event Aggregation Rules
ARF	Asset Reporting Format (used in conjunction with event payload data)	VII	Event Results
???	Event Management Policy Language	VIII	Event Management Policy
???	Common Event Type Enumeration	IX	Event Type Enumeration

** Specifications are only required for defining the data exchange components of generic EMAP workflow.*

EMAP Specs plugged into workflow